使用FlexConnect的外部Web驗證本地交換部署指南

目錄

簡介

本文檔介紹如何針對不同的Web策略將外部Web伺服器與FlexConnect本地交換配合使用。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- 有關FlexConnect架構和接入點(AP)的基本知識
- 瞭解如何設定和配置外部Web伺服器
- 瞭解如何設定和配置DHCP和DNS伺服器

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 執行韌體版本7.2.110.0的Cisco 7500無線LAN控制器(WLC)
- Cisco 3500系列輕量型存取點(LAP)
- 承載Web驗證登入頁面的外部Web伺服器
- 本地站點上的DNS和DHCP伺服器，用於向無線客戶端分配地址和IP地址

本文中的資訊是根據特定實驗室環境內的裝置所建立。雖然此部署指南使用7500系列WLC，但2500、5500和WiSM-2 WLC都支援此功能。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

功能概述

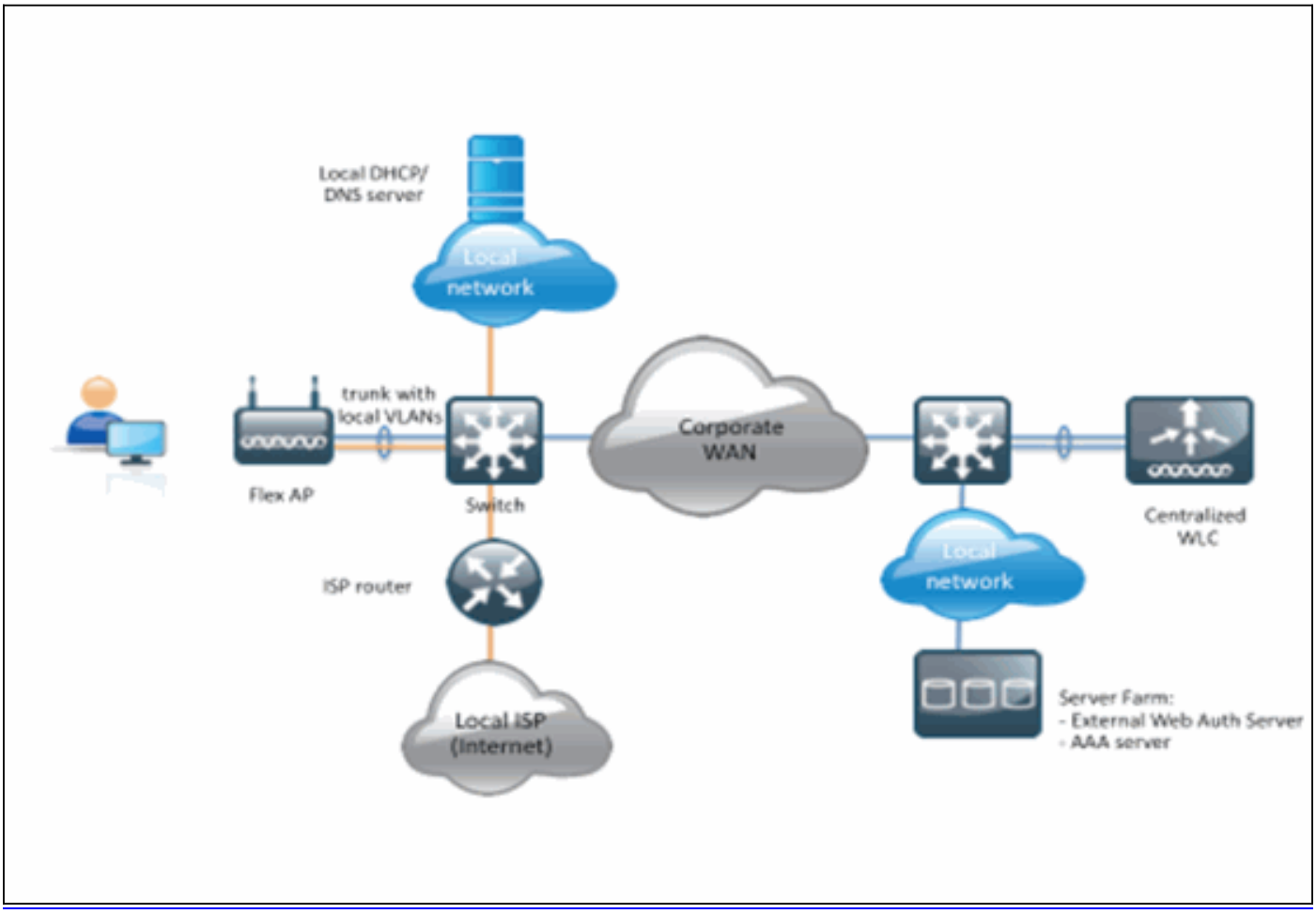
對於具有本地交換流量的WLAN（FlexConnect — 本地交換），此功能將執行Web驗證的功能從FlexConnect模式中的AP擴展至外部Web伺服器。 在WLC 7.2.110.0版之前，本地模式或FlexConnect模式的AP支援使用中央交換流量（FlexConnect — 中央交換）的WLAN外部伺服器的Web驗證。

此功能通常稱為外部Web驗證，它擴展了FlexConnect本地交換WLAN的功能，以支援控制器當前提供的所有第3層Web重新導向安全型別：

- Web驗證
- Web傳輸
- Web條件式重新導向
- 啟動顯示頁面條件式重新導向

考慮針對Web驗證和本機交換設定的WLAN，此功能背後的邏輯是直接在AP層級（而不是WLC層級）分佈和套用預先驗證FlexConnect存取控制清單(ACL)。透過這種方式，AP會在本地交換來自ACL允許的無線使用者端的封包。不允許的封包仍會透過CAPWAP通道傳送到WLC。另一方面，當AP通過有線介面接收流量時（如果ACL允許），會將其轉發到無線客戶端。否則封包會被捨棄。一旦使用者端通過驗證和授權，預先驗證FlexConnect ACL就會移除，而且所有使用者端資料流量都會允許並在本地交換。

注意：此功能在假設客戶端可以從本地交換VLAN到達外部伺服器的情況下工作。



摘要:

- 為FlexConnect本地交換和L3安全配置了WLAN
- FlexConnect ACL將用作預身份驗證ACL
- FlexConnect ACL一旦配置，必須通過Flex Group或單個AP推送到AP資料庫，或者應用於

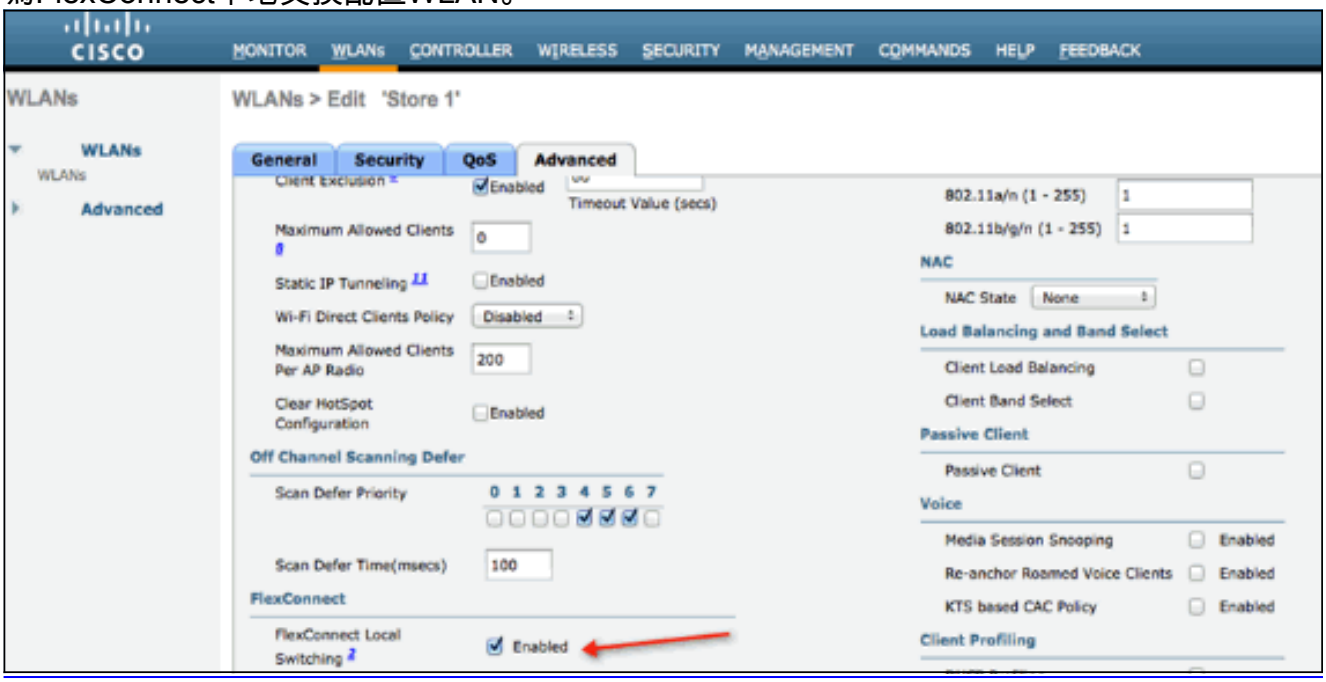
WLAN

- AP允許在本地交換與預身份驗證ACL匹配的所有流量

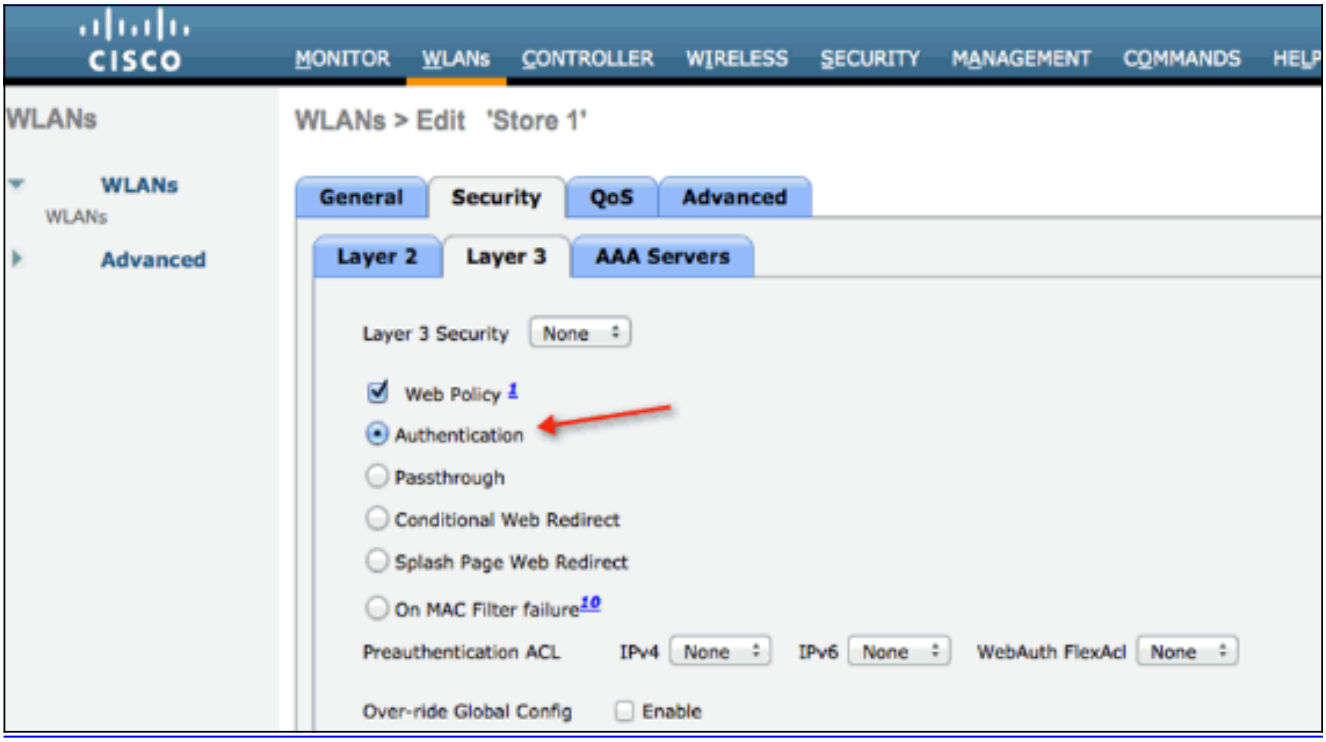
過程：

完成以下步驟即可設定此功能：

1. 為FlexConnect本地交換配置WLAN。



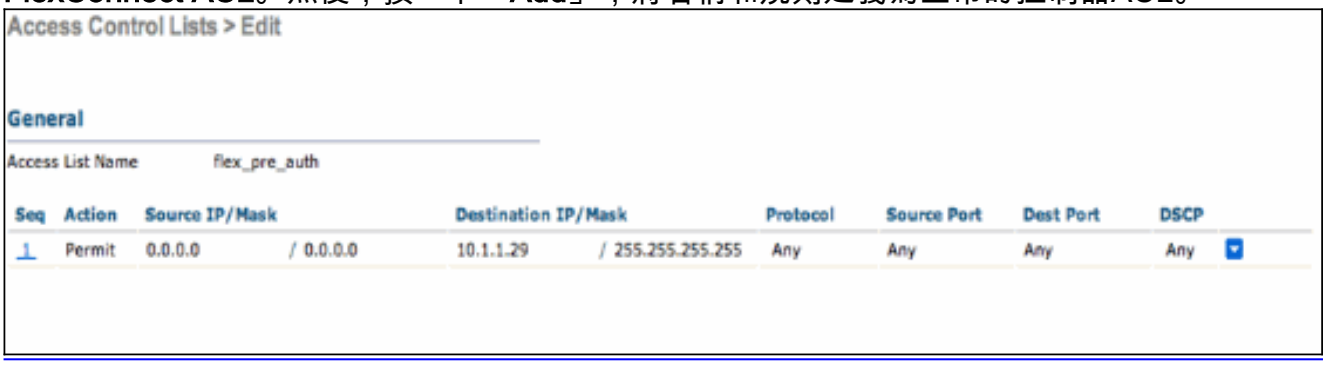
2. 若要啟用外部Web驗證，需要將Web原則設定為本地交換WLAN的安全原則。其中包括以下四個選項之一：驗證傳輸條件式 Web 重新導向啟動顯示頁面 Web 重新導向本檔案擷取Web驗證的一個範例：



前兩種方法類似，從配置角度可分為Web身份驗證方法。第二兩個（條件重定向和啟動頁）是Web策略，可以分組為Web策略方法。

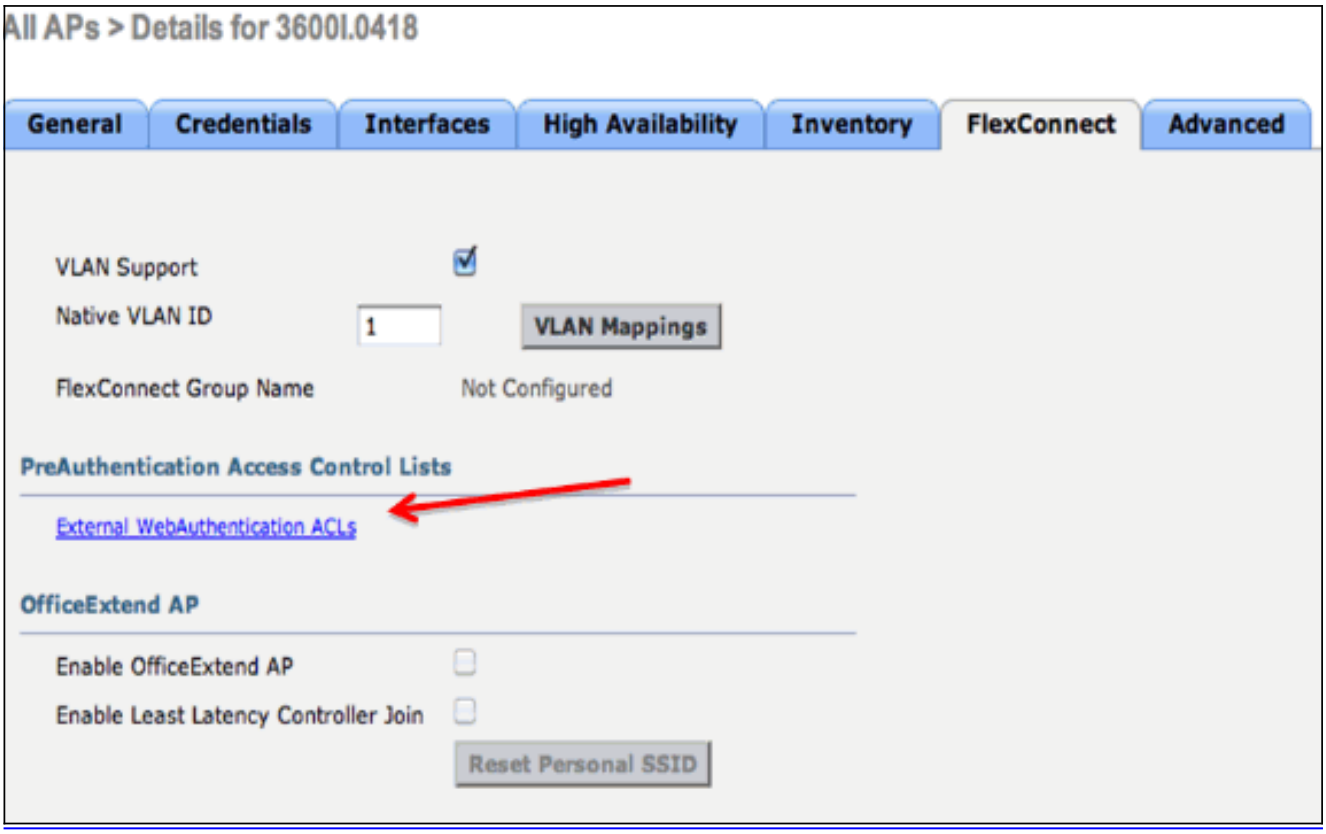
3. 需要配置預身份驗證FlexConnect ACL，以允許無線客戶端到達外部伺服器的IP地址。自動允許ARP、DHCP和DNS流量，不需要指定。在Security > Access Control List下，選擇

FlexConnect ACL。然後，按一下「Add」，將名稱和規則定義為正常的控制器ACL。

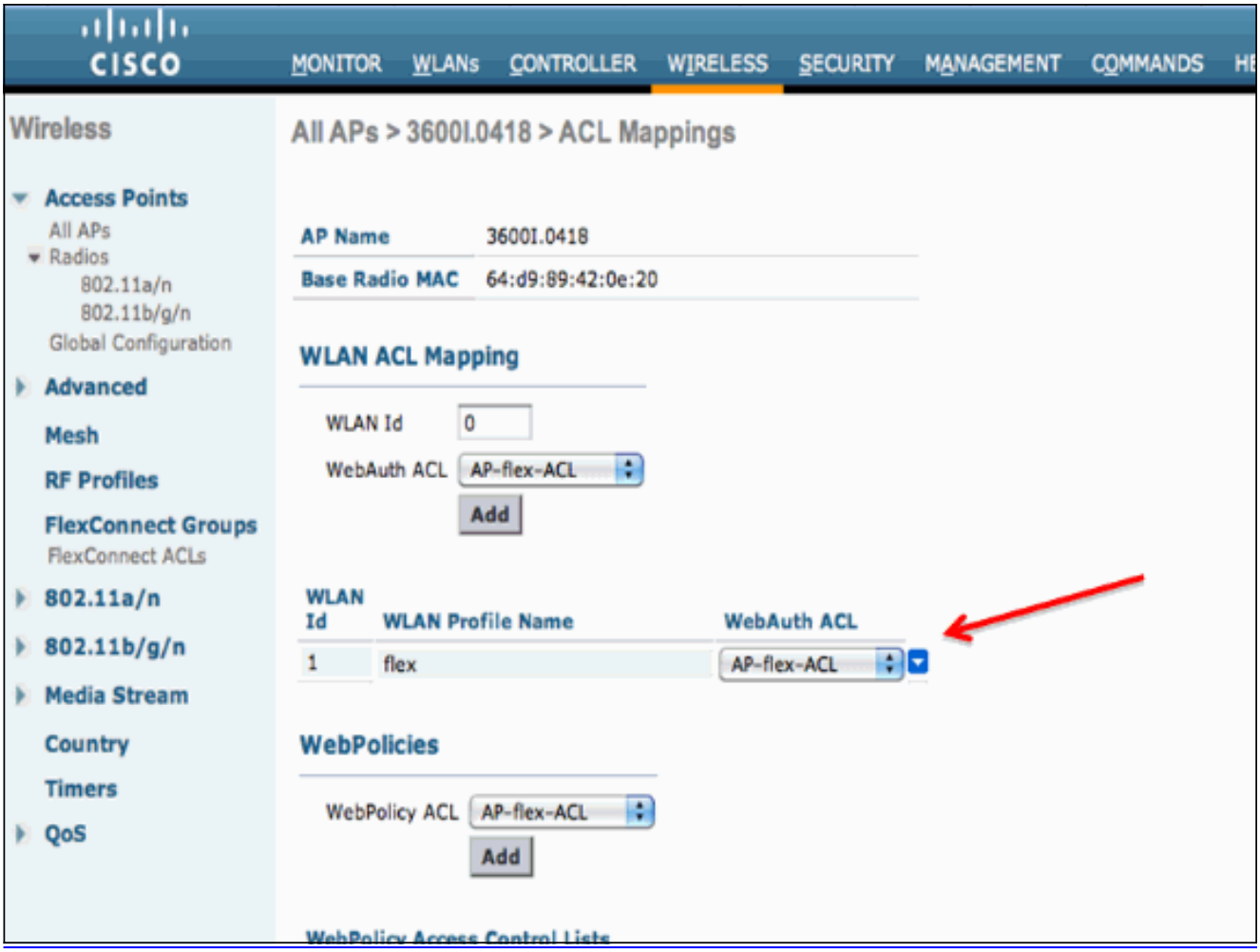


附註：您每次都需要為流量建立反向規則。

4. 建立FlexConnect ACL後，應該應用它，它可以在不同的級別執行：AP、FlexConnect組和WLAN。最後一個選項（WLAN中的Flex ACL）僅用於Web驗證和Web傳遞在Web原則下的其他兩種方法，例如條件式和Splash Redirect。ACL只能應用於AP或Flex組。以下是在AP級別分配的ACL示例。轉到**Wireless > select AP**，然後按一下**FlexConnect**頁籤：

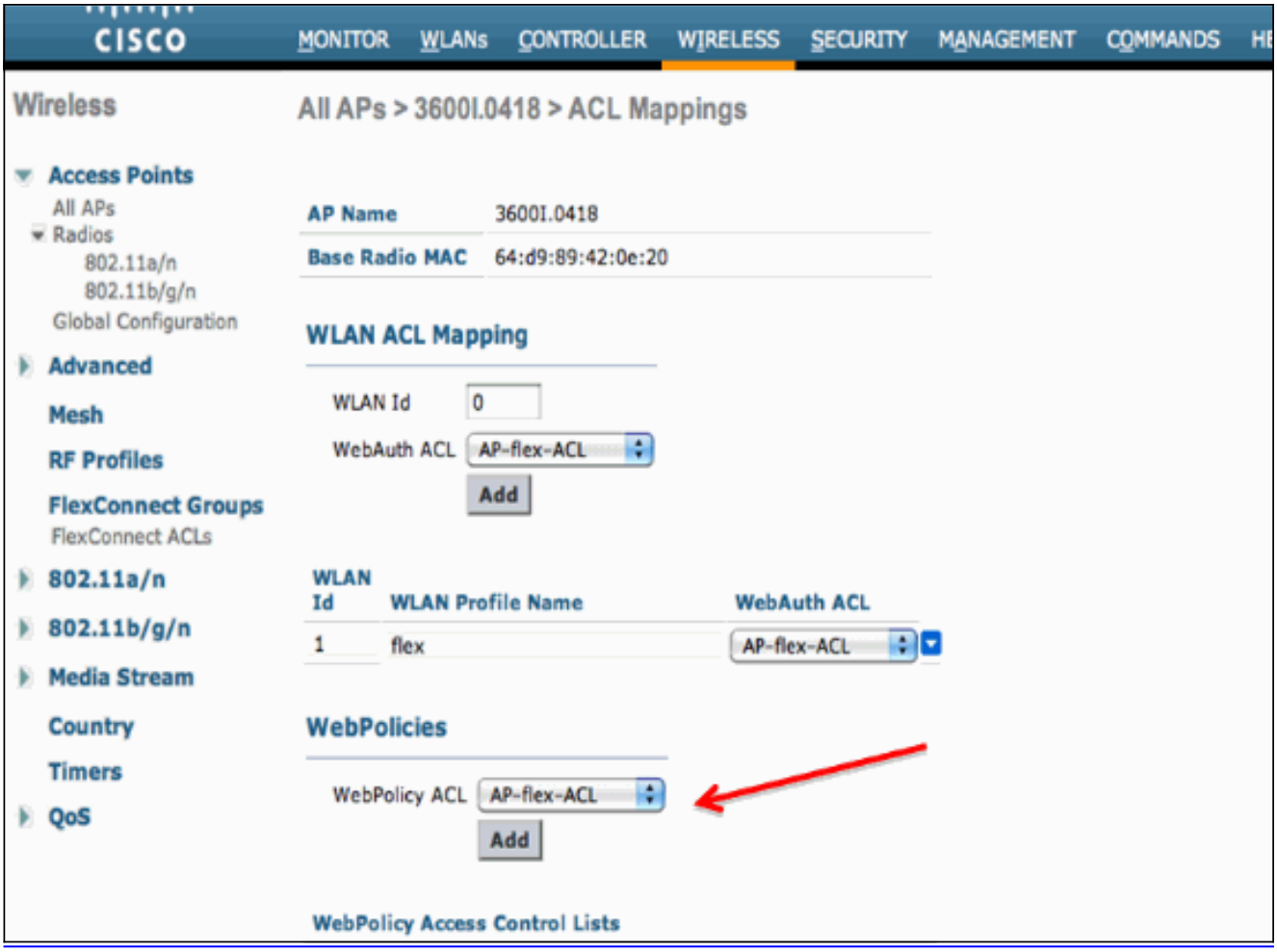


按一下**External WebAuthentication ACLs**連結。接下來，選擇特定WLAN Id的ACL:

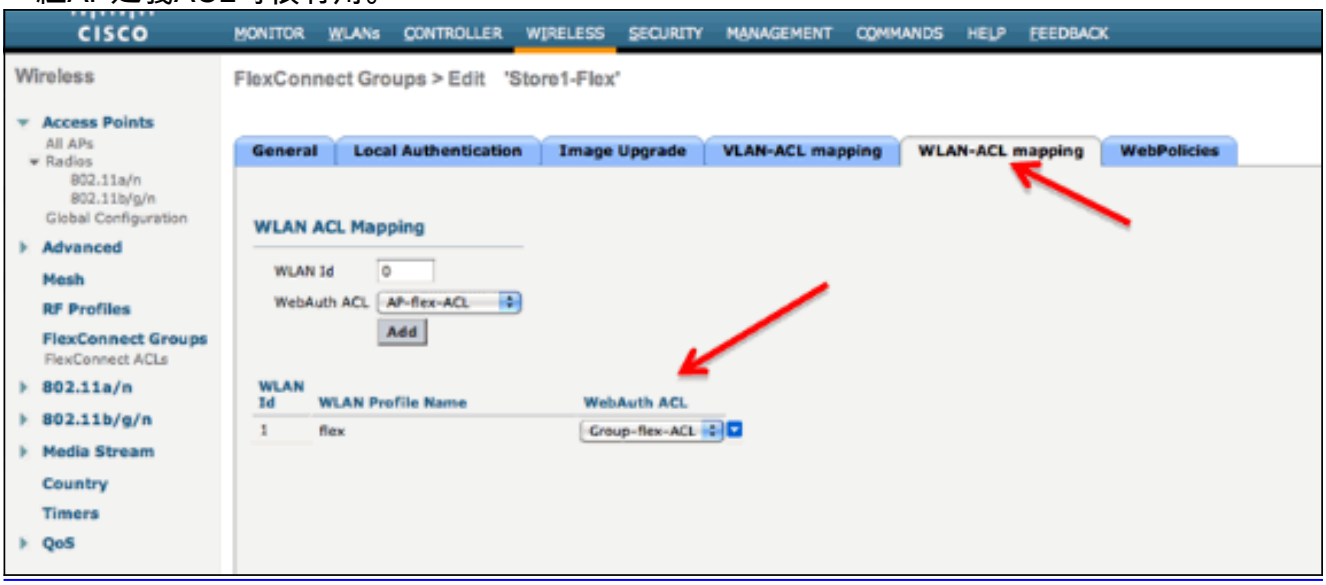


同樣地，對於Web策略ACL（例如，條件式重新導向或啟動顯示頁面重新導向），在按一下相同的外部WebAuthentication ACL連結後，您會收到在WebPolicies下選擇Flex Connect ACL的選項。如下所示

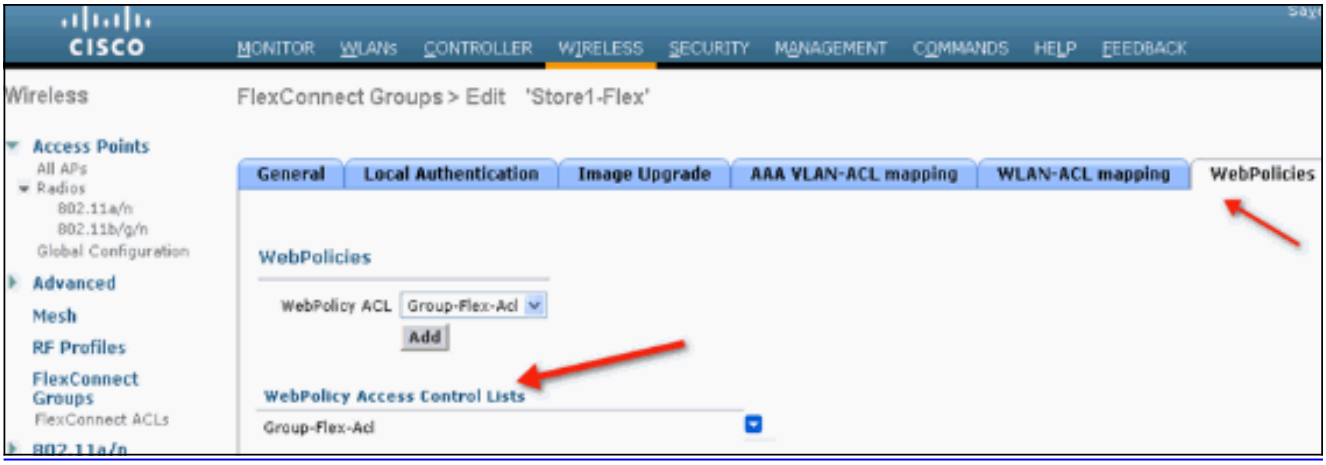
：



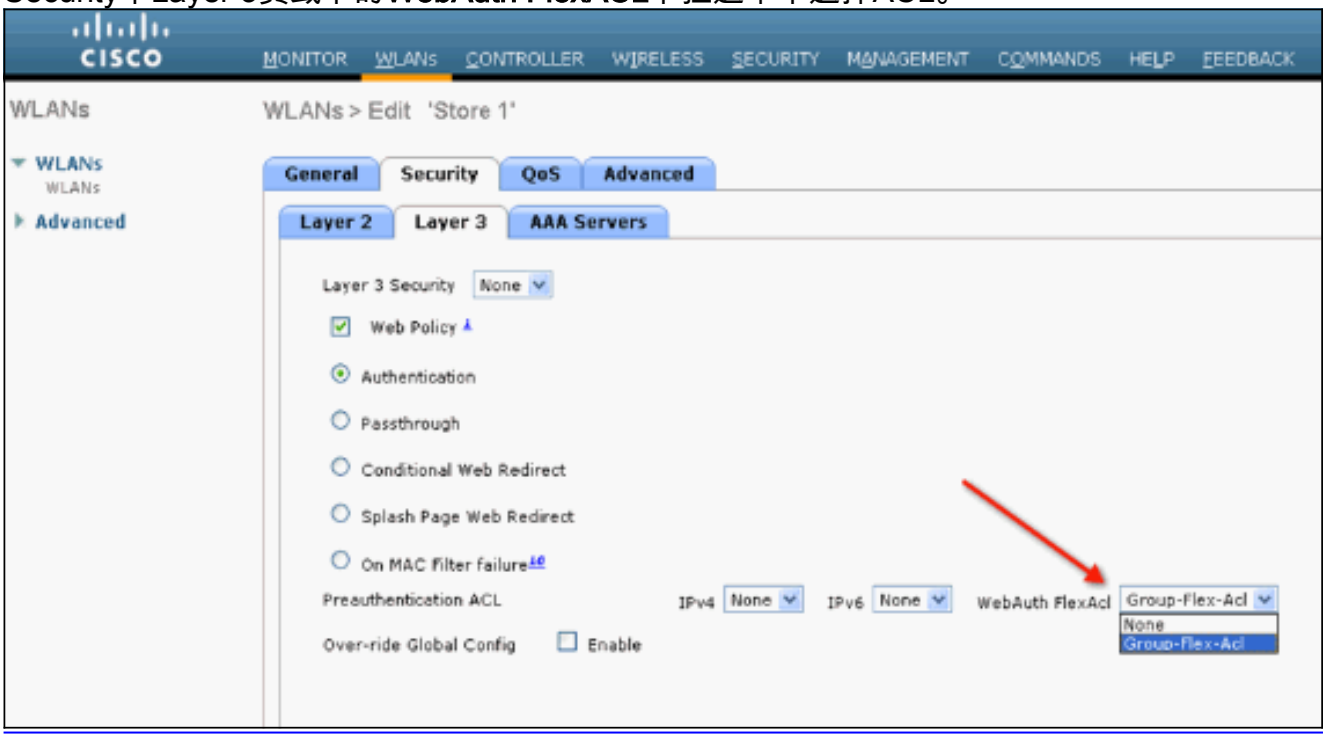
5. ACL也可以應用於FlexConnect組級別。若要執行此操作，請轉到FlexConnect組配置中的**WLAN-ACL對映**頁籤。然後，選擇要應用的WLAN Id和ACL。按一下「**Add**」。這在您希望為一組AP定義ACL時很有用。



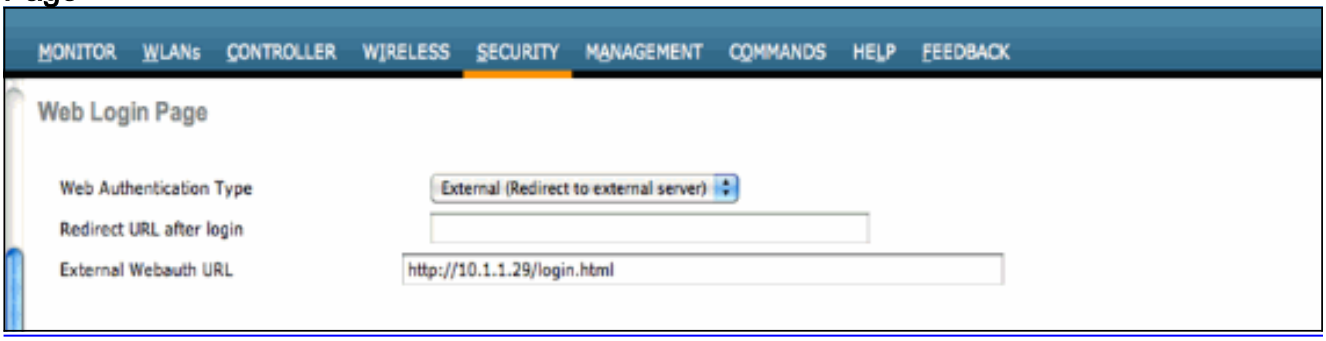
同樣，對於Web策略ACL（對於Conditional和Splash Page Web Redirect），您需要選擇**WebPolicies**頁籤。



6. Web驗證和Web傳輸Flex ACL也可以套用在WLAN上。若要執行此操作，請從WLAN > Security中Layer 3頁籤下的**WebAuth FlexACL**下拉選單中選擇ACL。



7. 對於外部Web驗證，需要定義重新導向URL。這可以在全域性級別或WLAN級別完成。對於WLAN級別，按一下**Over-ride Global Config**複選標籤並插入URL。在全域層級，前往**Security > Web Auth > Web Login Page**:



限制：Web驗證（內部或外部伺服器）要求Flex AP處於連線模式。如果Flex AP處於獨立模式，則不支援Web身份驗證。Web驗證（內部或外部伺服器）只支援中央驗證。如果為本地交換配置的WLAN配置為本地身份驗證，則無法執行Web身份驗證。所有Web重新導向在WLC執行，而不是在AP層執行。

相關資訊

- 技術支援與文件 - Cisco Systems